

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10214255 A**

(43) Date of publication of application: **11 . 08 . 98**

(51) Int. Cl. **G06F 15/00**
G06F 12/14

(21) Application number: **09018039**

(22) Date of filing: **31 . 01 . 97**

(71) Applicant: **FUJI XEROX CO LTD**

(72) Inventor: **CHIBA KENJI**
KIYOUJIMA HITOKI

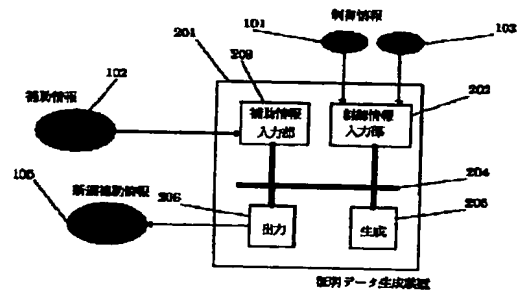
(54) METHOD AND DEVICE FOR GENERATING CERTIFICATION DATA

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a certification data generation technique for changing limit information such as the generation condition of an authority at a user's side.

SOLUTION: Auxiliary information 102 is inputted from an auxiliary information inputting part 203, and control information 101 corresponding to the auxiliary information 102 is inputted to a control information inputting part 202. Moreover, a user inputs new control information to the control information inputting part 202. The inputted control information and auxiliary information is transmitted through a data bus 204 to an auxiliary information generating part 205. The auxiliary information generating part 205 calculates new auxiliary information from the transmitted control information and auxiliary information based on a prescribed expression, and transmits the result through the data bus 204 to an auxiliary information outputting part 206. The auxiliary information outputting part 206 outputs the transmitted new auxiliary information 105.

COPYRIGHT: (C)1998,JPO



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平10-214255

(43)公開日 平成10年(1998) 8月11日

(51)Int.Cl.⁶

G 0 6 F 15/00
12/14

識別記号

3 3 0
3 1 0

F I

G 0 6 F 15/00
12/14

3 3 0 Z
3 1 0 D

審査請求 未請求 請求項の数13 O L (全 13 頁)

(21)出願番号 特願平9-18039

(22)出願日 平成9年(1997) 1月31日

(71)出願人 000005496

富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者 千葉 健司

神奈川県足柄上郡中井町境430 グリーン
テクなかい 富士ゼロックス株式会社内

(72)発明者 京嶋 仁樹

神奈川県足柄上郡中井町境430 グリーン
テクなかい 富士ゼロックス株式会社内

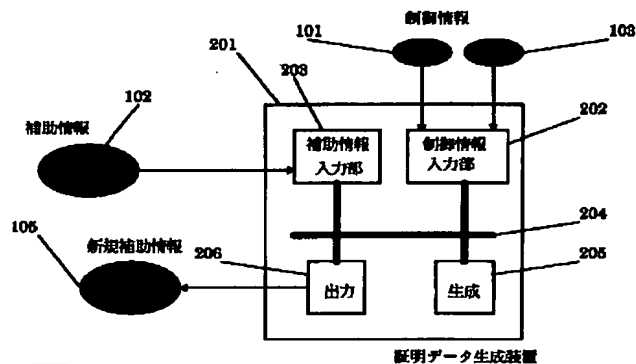
(74)代理人 弁理士 澤田 俊夫

(54)【発明の名称】 証明データ生成方法および装置

(57)【要約】

【課題】 権利の発生条件等の制限情報を使用者側で変更できるようにした証明データ生成技術を提供することを目的としている。

【解決手段】 補助情報102を補助情報入力部203から入力するとともに、補助情報102に対応する制御情報101を制御情報入力部202に入力する。さらに利用者が新規の制御情報を制御情報入力部202に入力する。入力された制御情報および補助情報はデータベース204を通じて、補助情報生成部205に送られる。補助情報生成部205は送られてきた制御情報と補助情報から新規補助情報を、所定の式に基づいて計算し、結果をデータベース204を通じて、補助情報出力部206に送る。補助情報出力部206は送られてきた新規補助情報105を出力する。



【特許請求の範囲】

【請求項 1】 入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成方法において、新たに設定したい制御情報と、現在の補助情報と、上記現在の補助情報を生成するのに用いた古い制御情報とに基づいて新たな補助情報を生成するステップと、上記新たな補助情報に基づいて新たな証明データを生成するステップとを有することを特徴とする証明データ生成方法。

【請求項 2】 上記補助情報は、上記制御情報と使用者の固有情報とに基づいて生成される請求項 1 記載の証明データ生成方法。

【請求項 3】 上記制御情報は権利の発生条件および証明データを生成するときの副作用を規定する請求項 1 または 2 記載の証明データ生成方法。

【請求項 4】 既存の制御情報を変更することによりあらたな制御情報を生成する請求項 1、2 または 3 記載の証明データ生成方法。

【請求項 5】 入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成装置において、上記制御情報を入力する手段と、上記補助情報を入力する手段と、入力された補助情報と、上記補助情報を生成するのに用いた制御情報と、新たに入力された制御情報とに基づいて新たな補助情報を生成する手段と、上記新たな補助情報に基づいて新たな証明データを生成する手段とを有することを特徴とする証明データ生成装置。

【請求項 6】 入力された制御情報を記憶する手段を設けた請求項 5 記載の証明データ生成装置。

【請求項 7】 入力された制御情報と補助情報の正当性を検証する手段を設けた請求項 5 または 6 記載の証明データ生成装置。

【請求項 8】 入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成装置において、上記制御情報を記憶する手段と、現在記憶されている制御情報に対応する補助情報を入力する手段と、上記現在記憶されている制御情報から新たな制御情報を生成する手段と、現在記憶されている制御情報と、現在記憶されている制御情報に対応する補助情報と、新たに生成された制御情報とに基づいて新たな補助情報を生成する手段と、上記新たな補助情報に基づいて新たな証明データを生成

する手段とを有することを特徴とする証明データ生成装置。

【請求項 9】 上記新たに制御情報を生成する手段は、制御情報の生成方法を制御する生成制御情報によって制御情報の生成の仕方を制御する請求項 8 記載の証明データ生成装置。

【請求項 10】 上記生成制御情報を使用回数の情報とし、使用回数と所定の値とを比較してその結果に応じて上記制御情報を変更する請求項 9 記載の証明データ生成装置。

【請求項 11】 上記生成制御情報を使用時間の情報とし、使用時間と所定の値とを比較してその結果に応じて上記制御情報を変更する請求項 9 記載の証明データ生成装置。

【請求項 12】 上記生成制御情報を記憶する手段を設けた請求項 9、10 または 11 記載の証明データ生成装置。

【請求項 13】 上記生成制御情報を入力する手段を設けた請求項 9、10、11 または 12 記載の証明データ生成装置。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、利用者の権利を証明するデータを生成する、証明データ生成方法および装置に関する。

【0002】

【従来の技術】 利用者の権利を制御するような技術としては、例えば特開平 4 - 1 5 7 5 5 5 号公報に記載されているものがある。この技術においては、利用者の ID と利用者の権利情報とをホストコンピュータに保持し、端末から入力される利用者の ID から利用者の権利情報を検索し、検索の結果得られた権利情報に応じた範囲で利用を許可し、所定のサービス提供の制御を行う。

【0003】 しかし前述の従来の技術においては、利用者の権利を変更するには、ホストコンピュータの情報を書き換えなければならない。したがって、変更作業はホストコンピュータの管理者が行う必要がある。そのため、大量の利用者情報を管理しなければならない場合、利用者情報の管理負荷がホストコンピュータおよびその管理者に集中してしまう。

【0004】

【発明が解決しようとする課題】 本発明は、以上の事情を考慮してなされたものであり、権利の発生条件等の制限情報を使用者側で変更できるようにした証明データ生成技術を提供することを目的としている。

【0005】

【課題を解決するための手段】 本発明においては、入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する構成において、利用者

側に、制御情報と補助情報とを用いて新たな補助情報を生成する手段を設けることで、上記の問題を解決するのである。すなわち、センタ側は利用者の基本的な権利情報（IDなど）のみを保持し、資源への利用権利の変更については、制御情報を利用者に与えるのみにすることができる。場合によっては利用権利の変更方法をあらかじめ利用者にもたせることも可能となるので、センタ側の負荷を低減することができる。

【0006】すなわち、本発明によれば、上述の目的を達成するために、入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成方法において、新たに設定したい制御情報と、現在の補助情報と、上記現在の補助情報を生成するのに用いた古い制御情報とに基づいて新たな補助情報を生成するステップと、上記新たな補助情報に基づいて新たな証明データを生成するステップとを行うようにしている。

【0007】この構成においては、利用者側において新たな制御情報を設定するのみで補助情報を変更することができ制御情報を変更する度に保持情報を利用者側に送る必要がなくなる。

【0008】また、この構成において、上記補助情報は、上記制御情報と使用者の固有情報とに基づいて生成されるようにでき、また、上記制御情報は権利の発生条件および証明データを生成するときの副作用を規定するものとすることができる。

【0009】副作用としては、証明データの生成（すなわち証明の結果例えばコンテンツを利用することになった場合には、その利用）に対する価格がある。これにより、利用量課金システムを実現できる。また、他の副作用としては例えば補助情報の有効期間がある。これにより、コンテンツ等の利用期間を規定できる。例えば、コンテンツ自体には利用期間を管理する機構を含めることなく、コンテンツの利用時間を補助情報の有効期間により間接的に管理できる。

【0010】また、既存の制御情報を変更することによりあらたな制御情報を生成するようにしてもよい。

【0011】また、本発明によれば、上述の目的を達成するために、入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成装置に、上記制御情報を入力する手段と、上記補助情報を入力する手段と、入力された補助情報と、上記補助情報を生成するのに用いた制御情報と、新たに入力された制御情報とに基づいて新たな補助情報を生成する手段と、上記新たな補助情報に基づいて新たな証明データを生成する手段とを設けるようにしている。

【0012】この構成においても、制御情報を変更する度に保持情報を利用者側に送る必要がなくなる。

【0013】また、この構成において、入力された制御情報を記憶する手段を設けてもよいし、入力された制御情報と補助情報の正当性を検証する手段を設けてもよい。

【0014】また、本発明によれば、上述の目的を達成するために、入力された認証用データと、少なくとも所定の制御情報に対応して生成された補助情報とに基づいて、使用者の権利を証明する証明データを生成する証明データ生成装置に、上記制御情報を記憶する手段と、現在記憶されている制御情報に対応する補助情報を入力する手段と、上記現在記憶されている制御情報から新たな制御情報を生成する手段と、現在記憶されている制御情報と、現在記憶されている制御情報に対応する補助情報と、新たに生成された制御情報とに基づいて新たな補助情報を生成する手段と、上記新たな補助情報に基づいて新たな証明データを生成する手段とを設けるようにしている。

【0015】この構成においても、制御情報を変更する度に保持情報を利用者側に送る必要がなくなる。

【0016】また、この構成において、上記新たに制御情報を生成する手段は、制御情報の生成方法を制御する生成制御情報によって制御情報の生成の仕方を制御するようにしてもよく、また、上記生成制御情報を使用回数の情報とし、使用回数と所定の値とを比較してその結果に応じて上記制御情報を変更するようにしてもよい。また、上記生成制御情報を使用時間の情報とし、使用時間と所定の値とを比較してその結果に応じて上記制御情報を変更するようにしてもよい。また、上記生成制御情報を記憶する手段を設けけもよく、上記生成制御情報を入力する手段を設けてもよい。

【0017】

【発明の実施の形態】

〔認証システムの概要〕まず、本発明の実施例について説明する前に、本発明の実施例が前提とする認証システムについて説明する。なお、本発明は、以下の認証システム以外にも適用可能である。

【0018】本発明の実施例が前提とする認証システムには、図1に示すように、3つのエンティティ、すなわち、管理センタ1、プロバイダ2、利用者3が存在する。プロバイダ2は、情報、装置、あるいは資源（以下コンテンツと総称する）をもち、それに対する利用者3のアクセスを制御したい。このような場合、公知の技術である公開鍵暗号技術を用いることができる。以下この公開鍵暗号技術の使用を前提にする。

【0019】公開鍵暗号技術にしたがって、各エンティティはそれぞれ以下のような情報を持つ。

管理センタ1 : センタの公開鍵ペア（e c, n c）、署名鍵d c（秘密）

利用者3 : 認証鍵d u（秘密）

プロバイダ2 : コンテンツ暗号鍵K（秘密）

管理センタ1の鍵はたとえばRSA (R i v e s t、S h a m i r、A d l e m a n) 暗号技術のような公開鍵暗号技術に基づいて作られる。利用者3は、 d_u を封入したトークンと呼ばれる利用者固有の認証装置(トークン)31と、コンテンツを利用するためのコンテンツ利用プログラム32とを持つ。基本的に利用者3はあるコンテンツに対してアクセスするため、アクセス制御を行う情報(以下チケットと呼ぶ)をセンタ1に発行してもらう。利用者はこのチケットと、トークンと呼ばれる利用者固有の認証装置31を用いて、資源へのアクセスが可能となる。

【0020】このチケット発行の準備として、以下のことが行われる。

【0021】まず、プロバイダ2は管理センタ1に依頼して、特定の資源に対する情報 n (以下これをチケット法数と呼ぶ)と E (チケット公開鍵と呼ぶ)を生成してもらう。 n は、暗号学的に安全な2つの素数 p 、 q を用いて、 $n=p \cdot q$ として、生成する。 n には、管理センタ1の電子署名が施される。さらに管理センタ1は E と n を保持する。プロバイダ2は自分のコンテンツを秘密の鍵 K を用いて暗号化する。この暗号化については慣用鍵暗号でも公開鍵暗号でもよい。次にプロバイダ2は E を用いて K を、

【0022】

【数1】 $K' = K^E \bmod n$

のように暗号化して、 K' を得る。そして、暗号化したコンテンツとともに利用者3に配布する。ここで、 K' は利用者3にはそれとわからない様にコンテンツ内に封入する。

【0023】利用者3はチケットを取得するため、自分のIDとチケット法数 n を管理センタ1に送る。管理センタ1は、利用者3のIDから検索した利用者3の秘密情報 d_u と、チケット法数 n とそれに対応するチケット公開鍵 E から生成した秘密情報 D を以下のように生成する。

【0024】

【数2】

$ED = 1 \bmod \phi(n)$ (1)

ただし $\phi(n)$ は n のオイラー数で、 p 、 q から生成される。

【0025】この D を用いて、チケット t を以下の様に生成し、利用者3に送る。

【0026】

【数3】

$t = D - F(d_u, L) + w\phi(n)$ (2)

ただし、ここで、 $w = G(d_u, L)$ 、 $G()$ は適当な*

$\Delta = F(d_u, L_{old}) - F(d_u, L_{new})$ (6)

に基づいて Δ を求める。次に求めた Δ を用いて、新しい補助情報 t_{new} を

$t_{new} = t_{old} + \Delta$

* 非衝突関数、 F は一方向性を持つ変換あるいは関数、 L は資源の利用条件等を記述した制御情報である。

【0027】利用者3は発行された t を用いて、コンテンツに以下のようにアクセスする。まず、利用者3は、乱数 r を生成し、以下のチャレンジ C を計算する。

【0028】

【数4】

$C = r^E \cdot K' \bmod n$ (3)

以上の計算はコンテンツ利用プログラム32内で行われる。

【0029】コンテンツ利用プログラム32はトークン31と通信し、 C をトークン31に送る。トークン31内では、

【0030】

【数5】

$R = C^{t \cdot F(d_u, L)} \bmod n$ (4)

を計算しコンテンツ利用プログラム32に戻す。

【0031】利用者3側では、コンテンツ利用プログラム32が R を用いて、

【0032】

【数6】

$K = r^{-1} \cdot R \bmod n$ (5)

により K を求め、コンテンツを復号化する。ここではじめて利用者はコンテンツの利用が可能となる。

【0033】以上、本発明の実施例の前提とする技術について説明した。以下、本発明の実施例について説明する。なお、以下に示す実施例では、前述のチケットを補助情報、 L を制御情報と考え、本発明による証明データ生成手法を前述のトークン内に実装する。このような構成をとることで、利用者は L をトークンに与えることで、新しいチケット t を得ることができる。

【実施例1】図2に本発明による証明データ生成手法の一実施例を示す。図2において、101は制御情報、102は制御情報101に対応した補助情報、103が新規制御情報、104は制御情報、補助情報、および、新規制御情報103とから新規補助情報を生成する補助情報生成手段、105は新たに生成される補助情報である。

【0034】この構成において、証明データ生成手段104は、与えられた制御情報101と新規制御情報103とを用いて、補助情報102を変更し、新規補助情報105として出力する。具体的には、すでに取得してある補助情報と制御情報をそれぞれ、 t_{old} 、 L_{old} 、新しい制御情報 L_{new} とし、

【0035】

【数7】

$\Delta = F(d_u, L_{old}) - F(d_u, L_{new})$ (6)

※【0036】

【数8】

(7)

のように生成する。

【0037】図3に実施例1を実現する証明データ生成装置の構成例を示す。この図において、制御情報101、補助情報102、新規制御情報103、および、新規補助情報105は図2と同様である。201は証明データ生成装置、202は外部から制御情報101、および新規制御情報103を入力する制御情報入力部、203は外部から補助情報を入力する補助情報入力部、204は入力された補助情報および制御情報を転送するデータバス、205は変更された制御情報と補助情報から新たな補助情報生成する補助情報生成部、206は生成された新規補助情報106を出力する補助情報出力部である。

【0038】この構成において、補助情報102を補助情報入力部203から入力するとともに、補助情報102に対応する制御情報101を制御情報入力部202に入力する。さらに利用者が新規の制御情報を制御情報入力部202に入力する。入力された制御情報および補助情報はデータバス204を通じて、補助情報生成部205に送られる。補助情報生成部205は送られてきた制御情報と補助情報から新規補助情報を、例えば前述の式(7)に基づいて計算し、結果をデータバス204を通じて、補助情報出力部206に送る。補助情報出力部206は送られてきた新規補助情報105を出力する。

【0039】図4は図3の証明データ生成装置の変形例を示す。図4において、制御情報101、補助情報102、新規制御情報103、新規補助情報105、証明データ生成装置201、制御情報入力部202、補助情報入力部203、データバス204、補助情報生成部205、および、補助情報出力部206は図3と同様である。301は入力された制御情報を記憶する制御情報記憶部である。

【0040】この構成において、入力された制御情報101はデータバス204を通じて制御情報記憶部301に送られ、保持される。次に新規の制御情報103が入力されると、記憶されている制御情報101を読み出して、データバス204を通じて補助情報生成部205に送る。この際、制御情報記憶部301内の制御情報103を新規制御情報105に置き換える。この場合置き換えず、記憶部内に新規制御情報を追加記憶するようにしても良い。このようにすることで、外部から入力される制御情報を用いず、記憶部内の制御情報のみを用いるようにすることもできる。さらに、コンテンツの利用と対応させることで利用履歴として取り扱い、例えば、利用状況に応じた課金や、さらに細かい制御情報の変更の制御を行う際に利用してもよい。

【0041】図5は図3の証明データ生成装置の他の変形例を示す。図4において、制御情報101、補助情報102、新規制御情報103、新規補助情報105、証明データ生成装置201、制御情報入力部202、補助

情報入力部203、データバス204、補助情報生成部205、補助情報出力部206、および制御情報記憶部301は図3と同様である。401は補助情報102の正当性を検査する検査部である。

【0042】この構成において、まず、補助情報については、発行時に管理センタがセンタ自身の電子署名をセンタの秘密鍵で行う。検査部401内ではセンタの公開鍵を用いて署名の検証を行う。さらに発行時に補助情報または制御情報が、正当な利用者のみが使用できるように、利用者の公開鍵を用いて暗号化したものを発行し、利用者は利用者の秘密鍵で復号化する。これにより、補助情報102の正当性を検証できる。

【0043】〔実施例2〕図6に本発明の証明データ生成手法の他の実施例を示す。図6において、制御情報101、補助情報102、新規制御情報103、補助情報生成手段104および、新規補助情報105は図1と同様である。501は制御情報生成手段である。

【0044】この構成において、最初に与えられた制御情報101を、補助情報生成手段104に送るとともに、制御情報生成手段501に送る。制御情報生成手段501は入力された制御情報を適当な条件に照らして書き換え、新規制御情報103を生成する。

【0045】図7に実施例2の証明データ生成手法を実現する証明データ生成装置の構成例を示す。図7において、制御情報101、補助情報102、新規制御情報103、新規補助情報105、証明データ生成装置201、補助情報入力部203、データバス204、補助情報生成部205、および、補助情報出力部206、制御情報記憶部301は図4と同様である。601は制御情報を変更して新規制御情報103を生成する制御情報生成部である。

【0046】全体の動作は図4と共通である。したがって構成上異なる制御情報生成部601の動作について説明する。制御情報生成部601は、データバス204経由で制御情報記憶部301から制御情報101を読み出し、所定の条件に従い制御情報101を変更し新規制御情報103を生成する。

【0047】図8に、図6における制御情報生成手段501(図7の制御情報生成部601)の動作を示す。図8において、制御情報101、新規制御情報103、制御情報生成部501は図6と同様である。701は制御情報の生成を制御する生成制御情報、702は生成の可否を決定する生成制御条件703は生成内容を規定する生成方法設定情報である。

【0048】この構成において、制御情報101が、制御情報生成部501に入力されると、その時点の条件を生成制御情報701内の生成制御条件702と比較し、所定の条件を満たせば、生成制御情報701内にあり、生成制御条件702に対応する生成方法設定情報703にしたがって制御情報101を変更し、新規制御情報1

03を生成し出力する。

【0049】図9に、図8における生成制御条件702に、使用回数を用いた動作例を示す。図9において、使用回数がそれぞれ n_1 、 n_2 、...、 n_k 以下のとき生成方法設定情報703が設定1、設定2、...、設定 k となるようにしている。生成方法設定情報703として、例えば1回あたりの使用単価を用いて、使用回数がある程度増えると、割引価格で使用できるようにすることができる。あるいは、生成方法設定情報703として、使用権限を設定に用いて、ある回数を使用すると使用不可能になるようにしてもよい。

【0050】図10に、図8における生成制御条件702に、使用時間を用いた動作例を示す。図10において、使用時間がそれぞれ t_1 、 t_2 、...、 t_k 以下の場合に生成方法設定情報703が設定1、設定2、...、設定 k となるようにしている。生成方法設定情報703として、例えば1回あたりの使用単価を用いて、使用時間がある程度増えると、割引価格で使用できるようにすることができる。あるいは、生成方法設定情報703として、使用権限を設定に用いて、ある期間使用すると使用不可能になるようにしてもよい。

【0051】図11に図7の制御情報生成部601の構成を示す。図11において、制御情報101、新規制御情報103、制御情報生成部、データベース204は図7と同様である。1001は、データベース204経由で制御情報と生成制御情報1003の入出力を行う入出力部、1002は、生成制御情報1003に基づいて、新規制御情報103を生成する生成部、1003は、新規制御情報の生成方法を規定する生成制御情報、1004は、内部データベースである。

【0052】この構成において、データベース204から、制御情報101、および、生成制御情報1003を、入出力部1001が読み込む。読み込んだ結果を生成部1002に送ると、生成部1002は生成制御情報を解読し、その結果に基づいて、制御情報101から新規制御情報103を生成する。新規制御情報103は、入出力部1001からデータベース204に出力される。

【0053】図12に図7の制御情報生成部601の構成を示す。図12において、制御情報101、新規制御情報103、制御情報生成部、データベース204入出力部1001、生成部1002、生成制御情報1003、内部データベース1004は図11と同様である。1101は、生成制御情報を記憶する生成制御情報記憶部である。

【0054】この構成において、新規制御情報103の生成方法は、図11と同様であるが、使用する生成制御*

* 情報1003を、生成情報記憶部1101から内部データベース1004経由で読み出して用いる。生成制御情報記憶部1101内部の生成制御情報1003は、データベース204、入出力部1001経由で外部から読み込んでも、例えばROMチップのような半導体に半永久的に書き込んだ形式で提供してもよい。

【0055】以上で実施例の説明を終了する。なお、本発明は上述の実施例に限定されるものではなく種々の変更が可能である。例えば、上述の実施例では補助情報を利用者の固有情報と制御情報とに基づくものとしたが、補助情報を制御情報のみに基づくものとしてもよい。

【0056】

【発明の効果】以上説明したように、本発明によれば、使用者側において、制御情報に基づいて補助情報が変更されるので、制御情報が変更される度にセンタ側から利用者に補助情報を送る必要がなくなる。

【図面の簡単な説明】

【図1】 本発明の実施例が適用される認証システムを説明する図である。

【図2】 本発明の実施例1の証明データ生成手法を説明する図である。

【図3】 実施例1を実現する証明データ生成装置の構成例を示すブロック図である。

【図4】 実施例1の証明データ生成装置の他の構成例を示すブロック図である。

【図5】 実施例1の証明データ生成装置の他の構成例を示すブロック図である。

【図6】 本発明の実施例2の証明データ生成手法を説明する図である。

【図7】 実施例2を実現する証明データ生成装置の構成例を示すブロック図である。

【図8】 実施例2の要部を説明する図である。

【図9】 実施例2の要部の動作を説明する図である。

【図10】 実施例2の要部の動作を説明する図である。

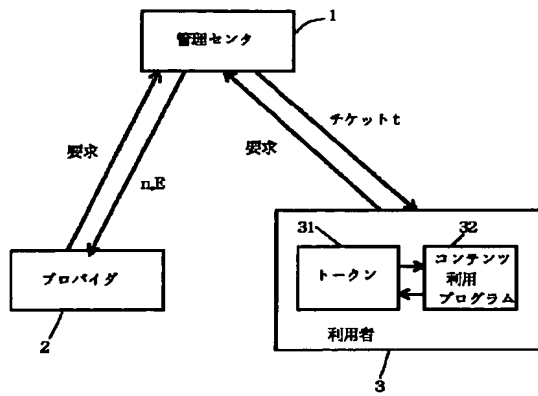
【図11】 図7の証明データ生成装置の制御情報生成部の構成例を示すブロック図である。

【図12】 図7の証明データ生成装置の制御情報生成部の他の構成例を示すブロック図である。

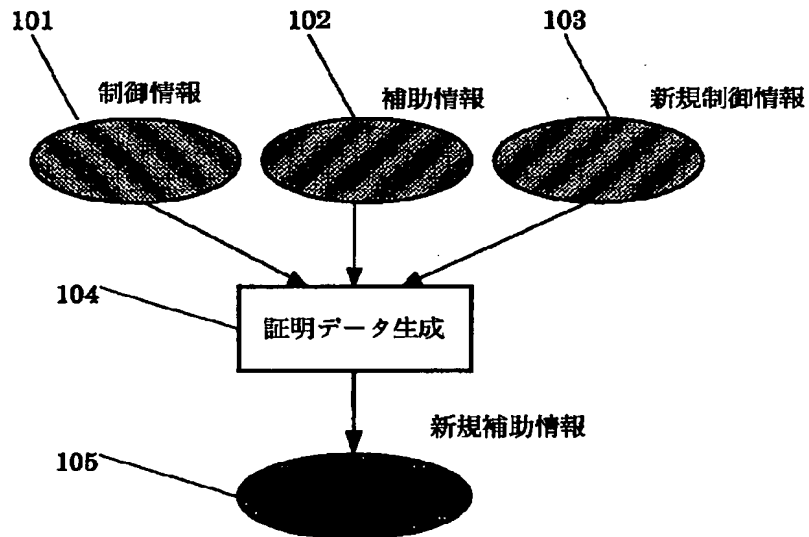
【符号の説明】

201 証明データ生成装置
202 制御情報入力部
203 補助情報入力部
205 補助情報生成部
206 補助情報出力部

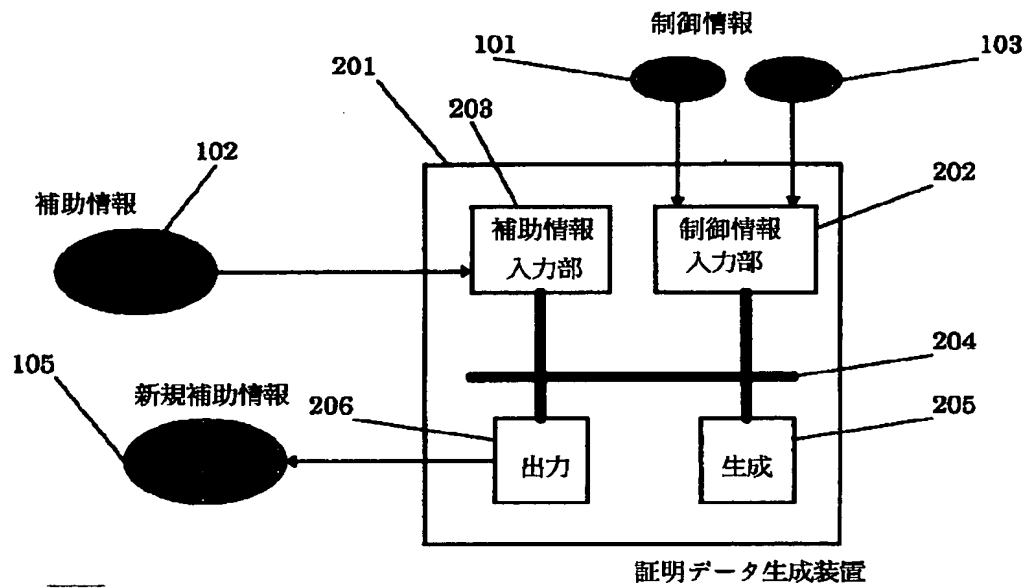
【図1】



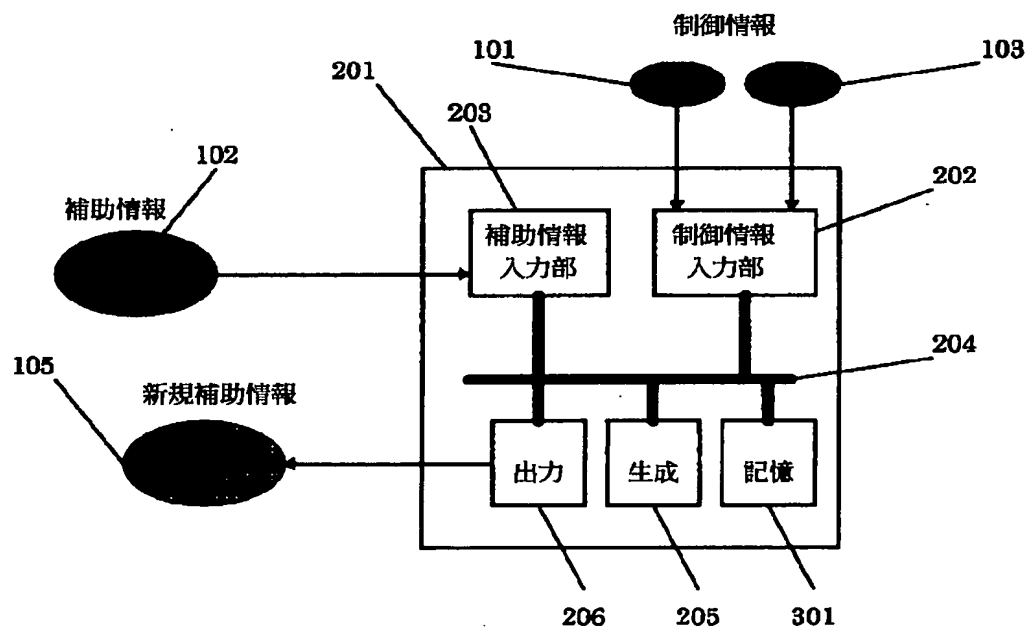
【図2】



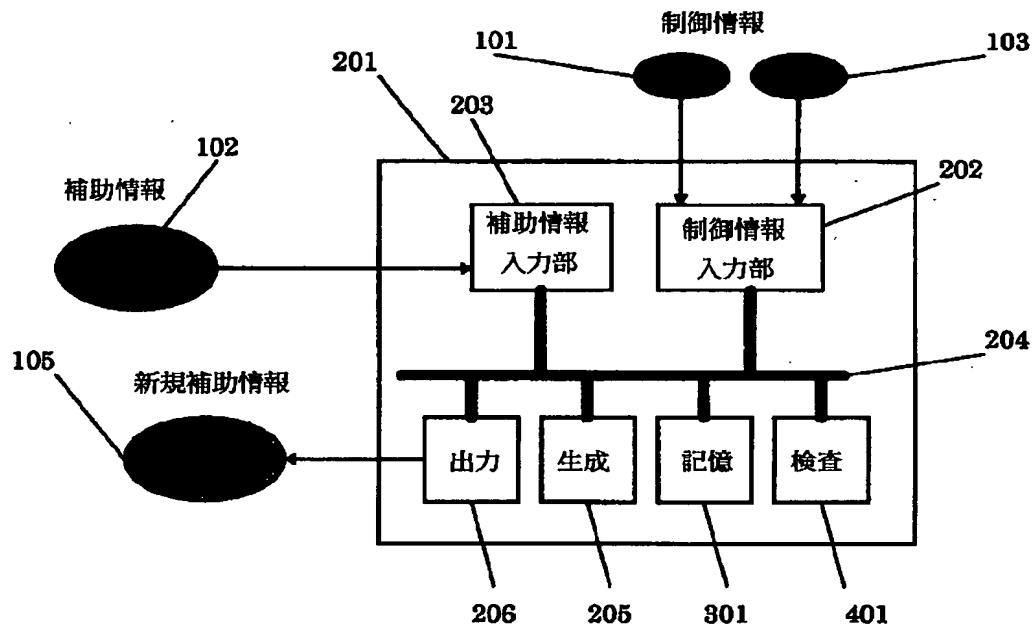
【図3】



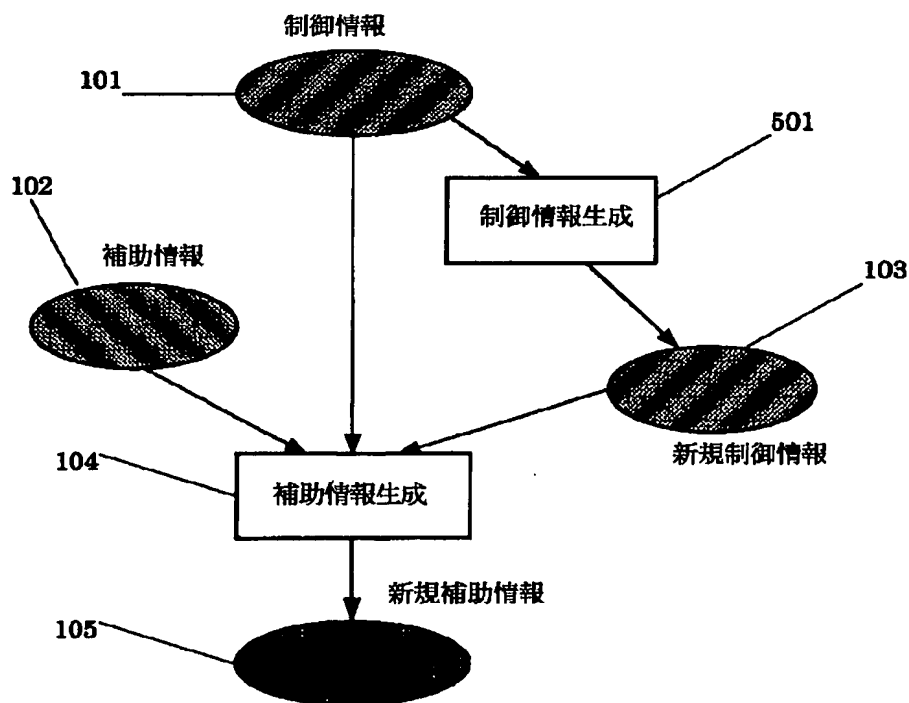
【図4】



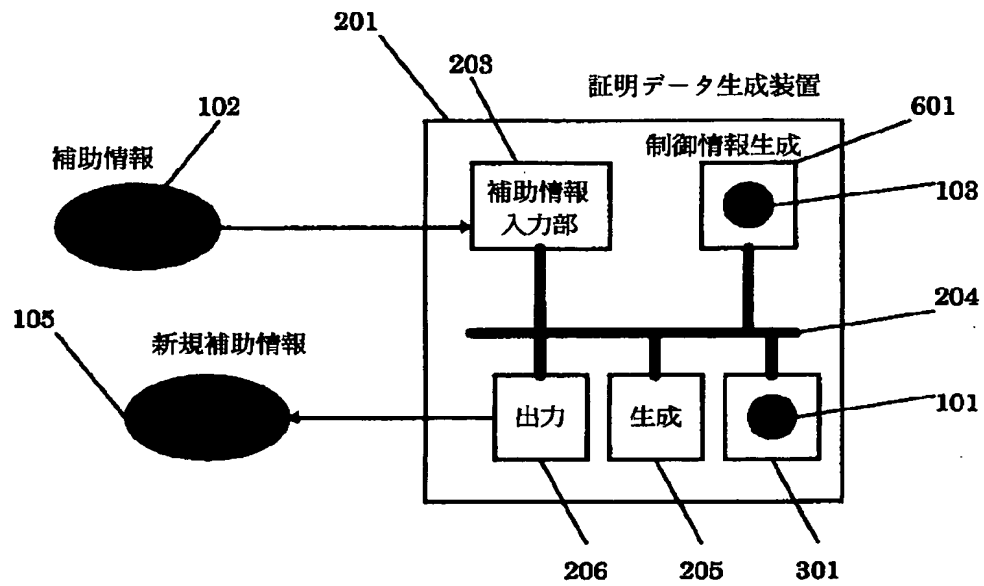
【図5】



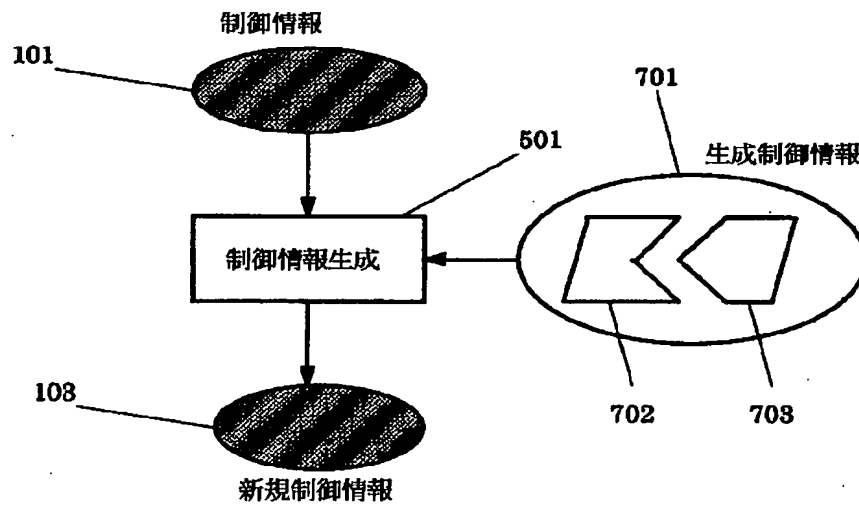
【図6】



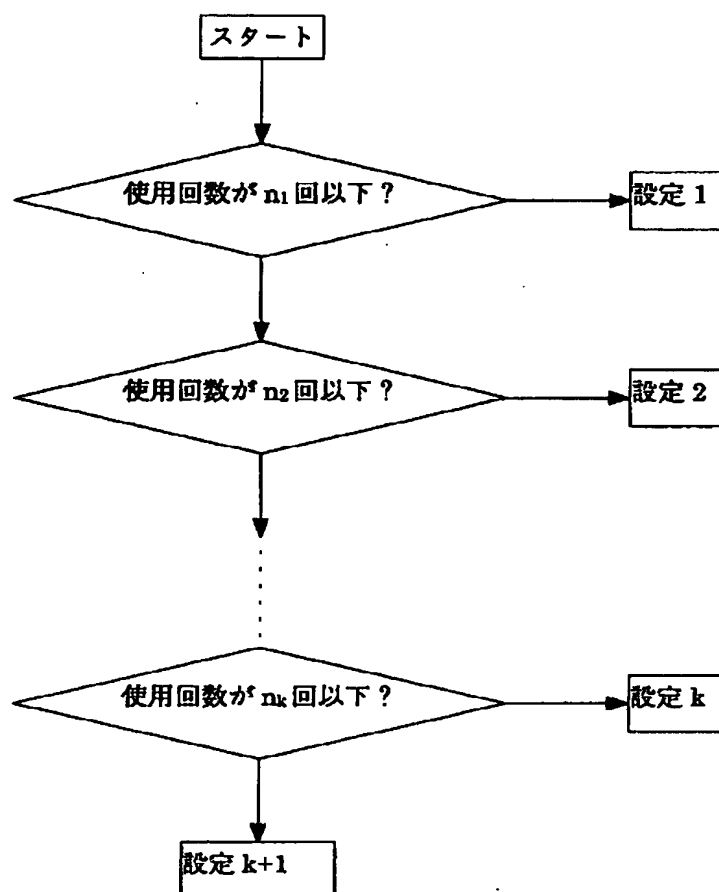
【図 7】



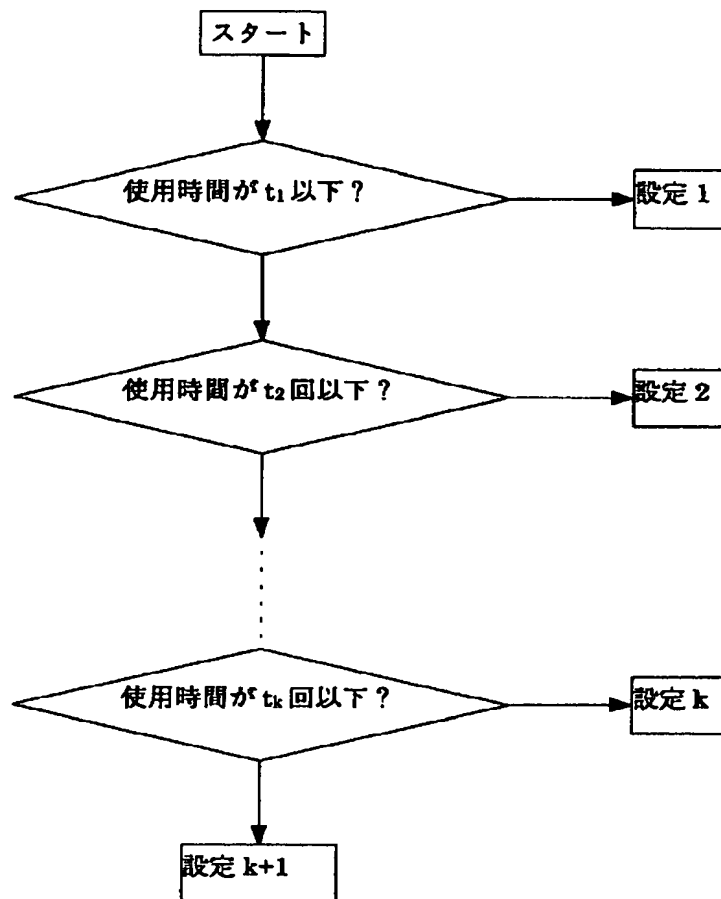
【図 8】



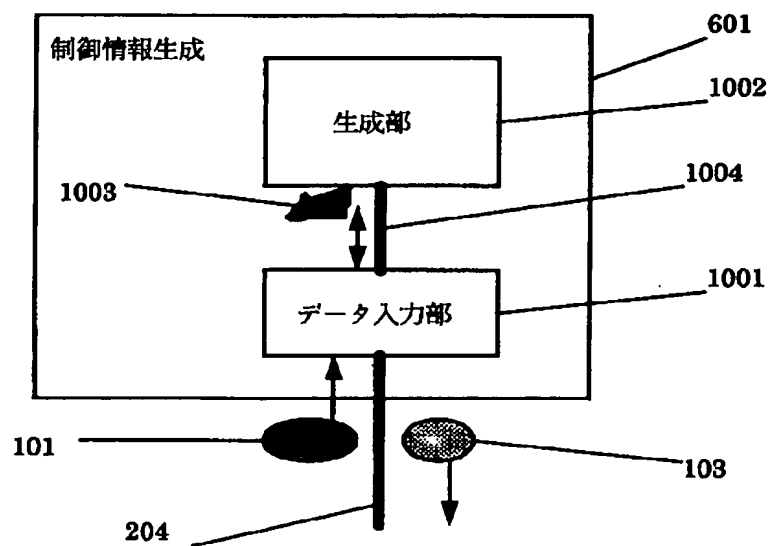
【図 9】



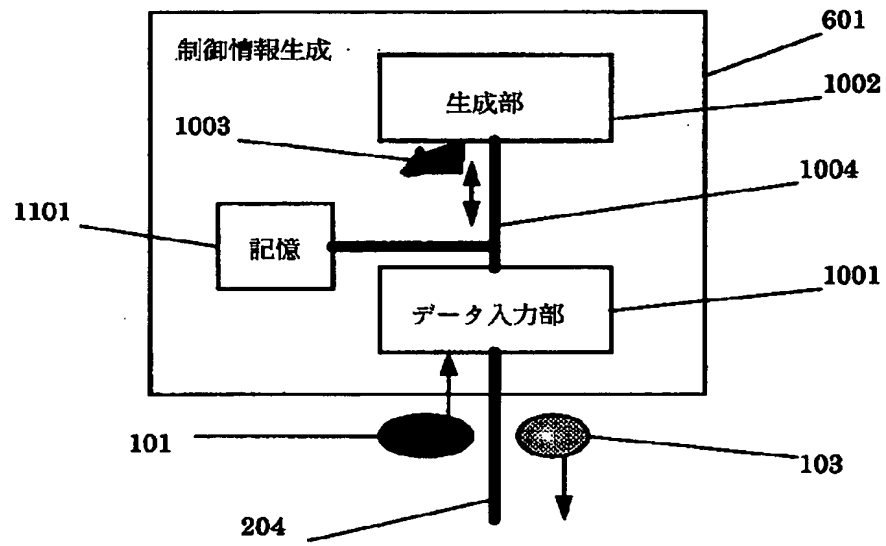
【図 10】



【図 11】



【図 12】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.